Oil and Gas

SOLUTION OVERVIEW

January 2016

CONVERGED TELECOMMUNICATION ARCHITECTURES FOR EFFECTIVE INTEGRATED PIPELINE OPERATIONS

Rik Irons-Mclean, Lead Architect Oil and Gas, IoE Vertical Solutions Group, Cisco Systems
José Zapico, Architect for Oil and Gas Pipeline and Upstream StruxureLabs, Smart Infrastructure, Schneider Electric

For more information,
contact Schneider Electric

Table of Contents

Chapter 1

Introduction

Oil and gas pipeline management is challenging, with pipelines often running over large geographical distances, through harsh environments, and with limited communications and power infrastructure available. In addition, pipelines must comply with stringent environmental regulations and operate as safely as possible, as well as addressing growing cyber and physical security threats.

Key pipeline requirements, however, have not changed. Pipeline integrity, safety, security, and reliability are essential elements that help operators meet demanding delivery schedules and optimize operational costs.

At the same time new operational and multiservice applications are enhancing the way assets and personnel operate. Modern cathodic detection, leak detection, intrusion detection, and physical security applications allow operators to reduce downtime, optimize production, and decrease energy
and maintenance costs. Real-time operational data access allows incidents to be identified and addressed quickly, or prevented from occurring in the first place.

Challenges must be addressed through a secure communications strategy to ensure operators can confidently rely on remote data, video, and collaboration solutions for safety and security in addition to operations.

Communications architectures, technologies, solutions, and management for process, energy, security, and multiservice applications must be robust, flexible, and scalable, and based on open standards, allowing operations from field device to enterprise levels by combining real-time process and business control automation, information management, energy management, and security with global supervision.

Pipeline requirements will vary depending on project, so it is essential that any communications solution be scalable and modular where elements can be interchanged without affecting fundamental architectural and operational functions. The technology choice for operational field telecoms should be viewed as a building block linking pipeline stations and control centers, and it must be flexible to meet end-user preferences including the possibility for future expansion.

Transmission pipelines are the key transport mechanism of the oil and gas industry, operating on a continuous basis outside of scheduled maintenance windows. Pipelines provide an efficient, safe, and cost-effective way to transport processed or unprocessed oil, gas, and raw materials and products both on- and offshore. It is essential that they operate as safely and efficiently as possible, and where problems occur they must be able to rapidly restore normal operation to meet environmental, safety, and quality requirements. To do so requires a unified solution including process and safety equipment for pipeline stations, as well as integrated monitoring, management, safety, and information systems for pipeline operations.

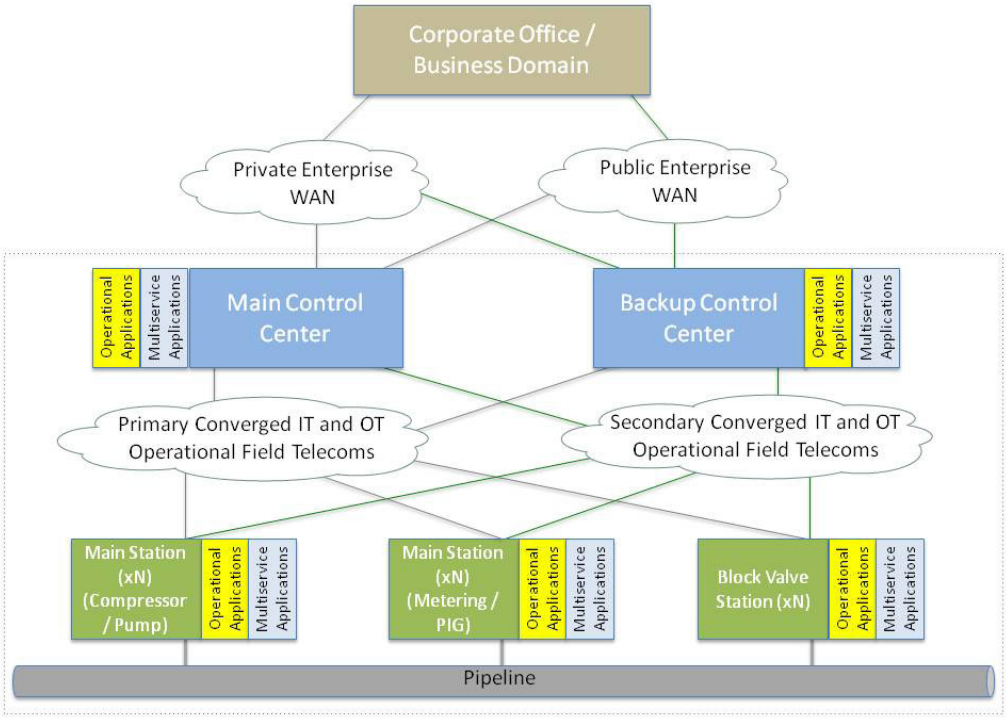

Figure 1. Oil and Gas Pipeline High-Level Architecture

Oil and gas pipelines (Figure 1) comprise a set of stations operating process, safety, and energy management functions geographically spread along the pipeline. Stations vary in size and function but typically include large compressor or pump stations, midsize metering, Pipeline Inspection Gauge (PIG) and terminal stations, and smaller block valve stations (Figure 2). Each process and application must be linked with the applications and processes at other stations, and at the control centers (main and backup) through an operational field telecoms infrastructure. (For further information about a virtualized power-efficient, space-saving, optimized design, refer to the "Integrated Enterprise Scada System Architectures for Safe and Efficient Pipeline Operations" solution overview paper.) The process must be done in a reliable and efficient way, avoiding communications outages and data losses. The control centers should also connected to the enterprise through a WAN to allow users to improve operational processes, streamline business planning, and optimize energy consumption.

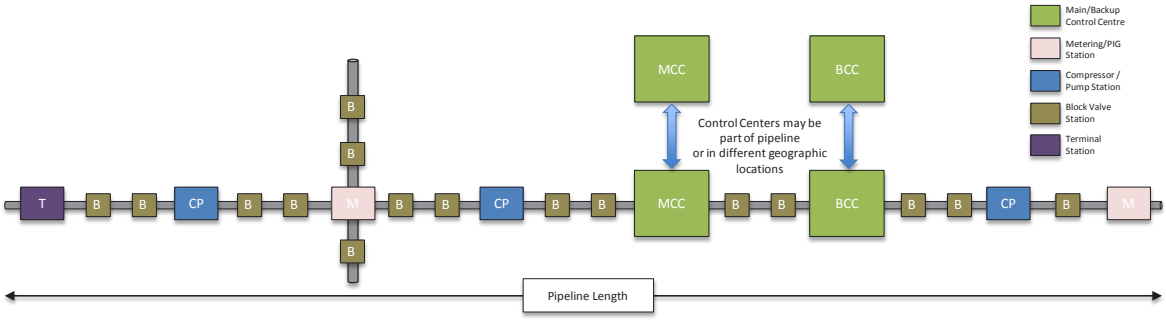

Figure 2. Example Pipeline Station Distribution

A jointly architected and validated approach to pipeline management and telecommunications (Figure 3) offers many realizable benefits. Solution integration quality and interoperability are maximized, while design and testing time are minimized. End users have a single point of reference accountable for integration and operational success from hardware, software, security, and management perspectives throughout a project lifecycle. The jointly architected design will provide maximum benefit for current operations, and be a platform for future application enablement and integration.

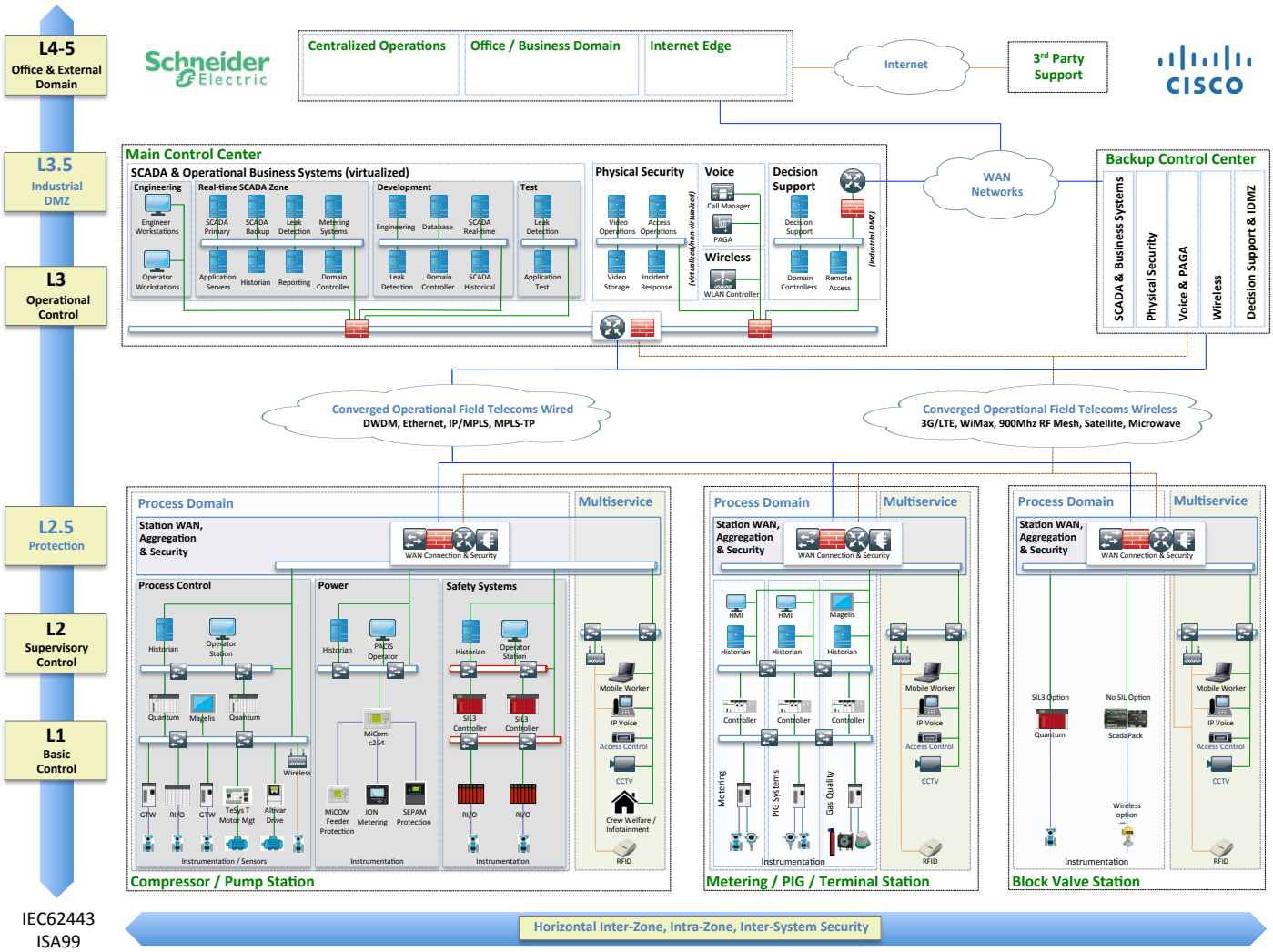

Figure 3. Cisco Schneider Pipeline Reference Architecture

Chapter 2

Pipeline Operational and Multiservice Applications

Pipelines consist of multiple applications and traffic types to support safe and efficient operations:

- Operational:
  - Supervisory Control and Data Acquisition (SCADA; A and B redundant systems)
  - Pipeline monitoring including leak detection, intrusion and tamper detection, earthquake detection, and PIG tracking; methods could include both traditional and more recent distributed acoustic sensors
  - Fluid management services including batch tracking and metering
  - Energy and power management and e-houses for the low-voltage applications
  - Security systems including closed-circuit television (CCTV) and video surveillance, access control, intruder detection, number plate recognition, and analytics
  - Telecoms including voice services (voice over IP [VoIP]), Public Address and General Alarm System (PAGA) safety system, hotline telephone system, and collaboration and video services
  - Industrial wireless sensor connectivity
- Business and residential:
  - Corporate traffic including voice, video, data, and email messaging
  - Residential services including worker infotainment, telephony, and wireless access
- Efficiency, planning, and optimization:
  - Supply-chain management for optimal logistics
  - Asset management for predictive maintenance, fleet, and nontraditional assets
  - Scheduling and planning for maintenance, turnaround and outages, and contractors
  - Intelligent alarm management
  - Management information systems to provide pipeline performance statistics

Applications can be categorized as operational (those directly involved with supporting pipeline operations such as the SCADA or leak-detection systems), and multiservice applications (either those that support pipeline operations such as video surveillance or those more concerned with business applications such as voice and corporate data).

Because of the critical nature of pipeline operational applications, there has often been a requirement for physical or logical separation of operational traffic from multiservice traffic at the station, over the field telecoms, or both. A well-designed modern telecoms network should be able to support physical, logical, or mixed implementations depending on the solution requirements. Key features of a design would include:

Pipeline management systems:

- Real-time or near-real-time control and supervision of operations along the pipeline through a SCADA system based in one or more control centers
- Accurate measurement of flow, volume, and levels to ensure correct product accounting
- Detection and location of pipeline leakage including time, volumes, and location distances
- Integrated security systems for personnel, the environment, and infrastructure using video surveillance, access control, and intrusion detection systems
- Assurance of safe operations through instrumentation and safety systems
- Energy management system to visualize, manage, and optimize energy consumption

Table 1. Operational Applications for Pipeline Operations

Application	Role
Schneider OASyS SCADA	Supervisory control and data acquisition located in the main and alternative control centers, providing system-level monitoring and control
Schneider Clear SCADA	Supervisory control and data acquisition located in the pipeline stations, providing local monitoring and control, feeding back to control centers
Schneider Wonderware InTouch	Distributed SCADA, with localized monitoring and control at station level, feeding back to control centers
Schneider PACiS	Digital control system for energy management system (EMS); station-level monitoring and control for power applications, feeding back to control centers
Schneider SimSuite	Pipeline and gas simulation, training, and forecasting system
Schneider Liquid Management System	Leak detection, batch tracking, metering, scheduling, ticketing, and tanking
Schneider Gas Measurement and Analysis System	Gas-system analysis
Schneider Endura	IP video management and video security surveillance
Cisco® Video Surveillance Operations Manager (VSOM), Cisco Physical Security Operations Manager (PSOM), Cisco Video Analytics, Cisco Physical Access Manager (Cisco PAM), and Cisco IP Interoperability and Collaboration System (IPICS)	Video surveillance, access control, analytics, and incident response management solutions

Operational telecoms infrastructure:

- High availability of communication for every asset along the pipeline:
  - Backup WAN services to ensure operational services continuation
  - Several primary and failover infrastructure connectivity options (Ethernet, Multiprotocol Label Switching [MPLS], dense wavelength-division multiplexing [DWDM], Optical Transport Network (OTN), cellular, wireless, etc.) depending on project requirements
- The ability to transport multiple traffic types across the same physical infrastructure:
  - Differentiated quality of service (QoS) between traffic types, helping ensure performance requirements of all operational traffic and multiservice traffic
  - Segregation capabilities (physical or logical) between services, helping ensure one traffic type does not affect another where designed
- Open standards for communication based on IP, with the ability to transparently integrate and transport traditional or older serial protocols
- Multilevel security to protect against cyber attacks and non-intentional security threats, and centralized configurable policy-based services
- Capability to integrate optional services to support pipeline operations such as VoIP, local Wi-Fi access, mobility, collaboration tools, and Internet access
- End-to-end communications network management, security management, and administration management—from the instrumentation or sensor to the control-center application
- Possible requirement at some locations for ruggedized equipment because of harsh conditions, local legislation, or industry certifications

Chapter 3

Communication Requirements

The communications network should be able to natively support many key standardized protocols (Table 2). Where older or traditional serial interfaces exist, the network should be capable of securely tunneling or encapsulating the data.

Table 2. Typical Key Protocols for Pipeline Applications

Ethernet- and IP-Based Protocols	Serial-Based Protocols
Modbus and TCP	Modbus
International Electrotechnical (IEC) 61850 Generic Object Oriented Station Event (GOOSE) (station), sampled value (SV) (station), and Manufacturing Message Specification (MMS)	
IEC 60870-104	IEC 60870-101
Distributed Network Protocol 3/IP (DNP3/IP)	DNP3
EtherNet/IP (industrial protocol)	
OLE for Process Control (OPC)	
TCP/IP	
FTP	
Proprietary protocols	Proprietary protocols

Timing for time-of-day occurrence, sequencing, and comparison for event analysis is essential, as well as synchronization technologies. Clock redistribution through mechanisms such as Network Time Protocol/Simple Network Time Protocol (NTP/SNTP), 1588 Precision Time Protocol (PTP), and 1 pulse per second (1PPP) should be built into the communications network infrastructure, as well as synchronous Ethernet.

Most pipeline management applications have historically required low bandwidth, with undemanding jitter and latency requirements. In essence these applications need to operate over low-bandwidth and lossy networks.

With the advent of newer WAN technologies, bandwidth restrictions have eased, and operational applications have emerged that require much higher bandwidth and lower latency and jitter requirements such as onshore real-time optical sensing for gas leaks. In addition, newer multiservice applications such as video surveillance and voice have also increased bandwidth requirements and put more strict requirements on jitter and latency.

The primary concern for any oil and gas network is high availability and reliability to ensure operations. However, with multiple applications coexisting on a communications network, dynamic bandwidth allocation, predictable and deterministic behavior, Differentiated Services (DiffServ), high capacity, and monitorable service-level agreements (SLAs) must be delivered to ensure the right applications operate in the right way at the right time.

To meet this redundancy and reliability, mechanisms are required at the physical, data, or network layer, or a combination for an operational WAN. This requirement should include sub-50-ms network reconvergence, traffic engineering for path selection and path redundancy, quality of service (QoS) for DiffServ and bandwidth reservation, and device redundancy.

Chapter 4

Security Considerations

The process-control domain has evolved greatly over recent years, with mechanical systems being replaced with analogue and then digital control mechanisms. As a result, new protocols have been introduced to allow communication between controllers and field devices, and to control centers. New communications networks have been introduced as a result, and the integration of multiservice applications has created an evolution in industrial networks to a point where they resemble enterprise networks much more closely. However, the requirements, operations, and concerns of industrial communications networks are markedly different for enterprise networks.

Historically security for the process-control domain was tackled through a "security by obscurity" approach. Networks were seen as standalone with no public access, proprietary protocols were seen as being difficult to understand and compromise, and security incidents were more likely to be accidental. Security measures have often assumed that if the location or access method of a vulnerable point isn't widely known it will not be exploited.

With the growing number of security incidents, customer best practice, regulation, and the integration of newer IT-based services, cyber security has become a top concern. Many countries have specific critical infrastructure programs that cover oil and gas, and more standardized approaches such as NERC-CIP are becoming applicable.

Not only is there a focus on securing operational applications across the WAN, but there is a need to consider other areas such as the coexistence of corporate data and residential worker traffic across a common operational WAN, secure remote access into the control-center environment and into the process domain, external third-party support, antivirus and patch management, and integration of new communications networks such as wireless infrastructure. The communications networks may also traverse public service provider networks rather than privately owned networks and therefore require additional layers of security.

It is recommended to follow an architectural approach to securing the process-control domain and associated WAN network. Recommended models would be the Purdue Model of Control Hierarchy and International Society of Automation 95 (ISA95)/ISA99 security levels. To help adhere to the requirements of IEC 62443 and achieve a robust solution for security and compliance, it is essential to use an end-to-end approach with technologies designed to operate together, minimizing risk and operational complexities (Figure 4).

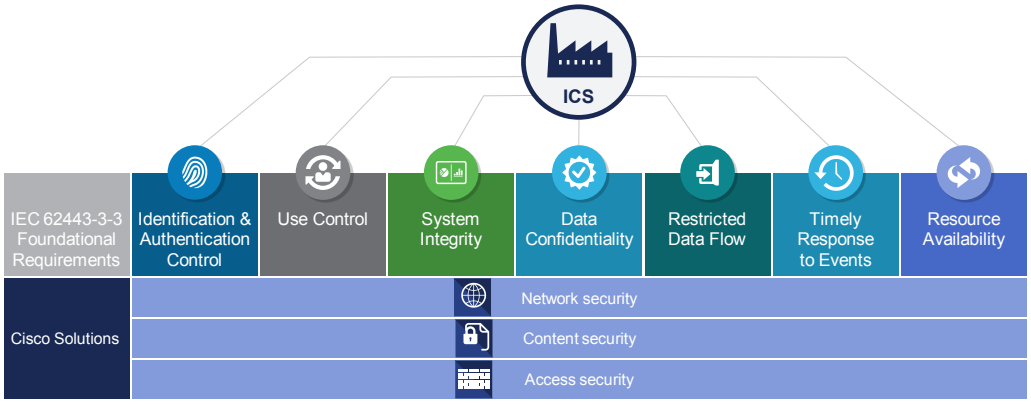

Figure 4. IEC 62443 Foundational Requirements

Taking an architectural approach to security will help secure the operational pipeline WAN against the critical security concerns (Figure 5).

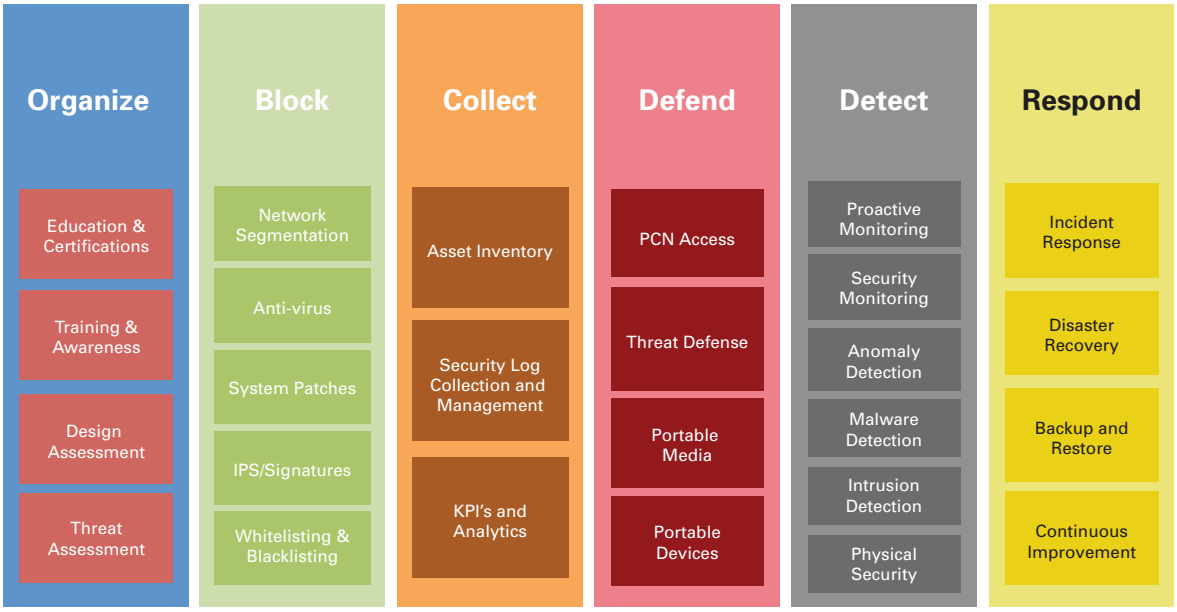

Figure 5. Cisco Risk Control Framework for Process Control Domains

Security services for the pipeline should include common security policies, management and context, transport security, network policy enforcement, research intelligence and threat defense, and physical security, leading to the important network architecture principles:

- **Access control:** Authentication and authorization of all personnel and devices
- **Data confidentiality and privacy:** Requirement that data privacy and data integrity for all operational and control data must be ensured (SCADA, automation, protection, etc.)
- **Threat detection and mitigation:** Protection of all critical assets
- **Integrity of platforms and devices:** Secure devices over the entire lifecycle

Chapter 5

Pipeline Communication Technology Options

Based on these application requirements, the correct choice of technology is imperative to architect a properly integrated pipeline management solution, and may vary depending on green- or brownfield deployments and power and footprint considerations.

Historical pipeline technologies have included direct telephone lines, microwave, cellular, and satellite links. These technologies are now proving inadequate or too expensive for some of the new capabilities that are needed. It is difficult or impossible to provide real-time pipeline condition data, frequent precise flow-measurement data, multiple security video feeds, and multiservice applications, making it harder to react to operational incidents, security incidents, or sabotage. At the same time new operational technologies to better detect and locate problems such as distributed acoustic sensors for leak detection and tamper detection, requirements to increase revenue by offering new business services such as service provider functions, and remote community services such as education and healthcare are influencing technology choice.

Where fiber connectivity is available, deployment options typically include Ethernet, IP, MPLS, and DWDM. Installing fiber also makes it possible to implement newer operational technologies such as distributed optical acoustic sensing for pipeline monitoring, as well as being able to use additional fiber pairs or wavelengths to provide revenue-generation services by leasing them.

Layer 2 Ethernet with Layer 3 Transport

Ethernet benefits in the LAN are well-understood, and this technology is rapidly evolving to provide the same benefits for Layer 3 applications across the WAN (Figure 6):

- **Scalability:** Ethernet is a proven technology with easy scalability options to meet the wide range of bandwidth requirements for a pipeline system, often without a change in onsite equipment. It can readily provide 100-Mb or -Gb connectivity between stations, and 10-Gb connectivity between control centers for normal operations or failover scenarios. The availability of standardized services independent of physical access type reduces complexity and cost.
- **Cost-effective:** The price per megabit of bandwidth is lower for Ethernet services in comparison to alternatives. Ongoing operational costs are typically lower for Ethernet, because the knowledge base for this technology is widely available within the industry.
- **Flexibility:** Ethernet provides a flexible WAN solution for pipeline operations and can interoperate with older technologies to enable a smooth migration path. It supports QoS, allowing operators to converge operational and multiservice data, video, and voice applications over a single WAN infrastructure and meet deterministic requirements.

- **Simplicity:** The industry is standardizing on Ethernet for the process control, energy management, and safety systems. With Ethernet-based services for the WAN, the network architecture is greatly simplified. This architecture is particularly attractive for certain applications such as distributed computing, data replication, and business continuity.
- **Expediting and enabling new applications:** New applications requiring high bandwidth and low latency that were previously not possible or prohibited by high cost are enabled, meeting current and future pipeline use-case deployment.

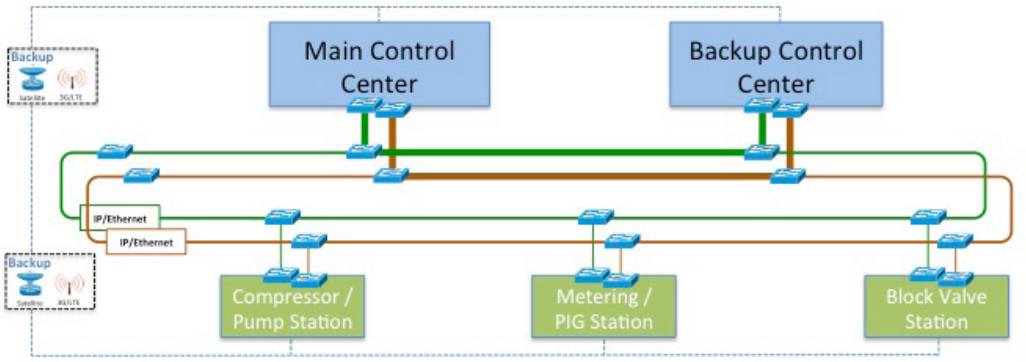

Figure 6. High-Level Ethernet-Based Pipeline Architecture

Many architectural and technical areas should be considered when deploying an Ethernet-based WAN for pipeline operations, as highlighted in Table 3.

Table 3. Technical Considerations When Deploying Ethernet

Benefits and Considerations
Layer 2 VLANs allow logical traffic separation between applications, providing security and supporting effective use of fiber pairs.
Ethernet provides good resiliency and redundancy options to ensure application SLAs are met.
Low-latency transport and sub-50-ms network reconvergence are possible using technologies such as Resilient Ethernet Protocol (REP) for ring topologies and Flexlink for tree and star topologies.
The operator's choice of Layer 3 routing protocols such as Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), and Intermediate System-to-Intermediate System (IS-IS) can be run across the Ethernet WAN to support all operational and multiservice applications.
Simplicity of deployment, configuration, and management makes initial rollouts quicker, and adds, moves, and changes easy.
Ethernet natively provides good support for multicast for applications such as video.
The QoS model allows you to prioritize some applications over others, and meet bandwidth, latency, and jitter requirements in a flexible manner.
The distance limitation between stations is 80 km maximum for connectivity without additional technologies.
Although Ethernet offers a potential for large broadcast or security vulnerability domains, these concerns are easily mitigated through architecture choice, technologies deployed, and security mechanisms.

The technology platform choice for an Ethernet-based WAN will depend on environmental, power, and space requirements, as well as technology preference by the pipeline operator (Table 4).

Table 4. Recommended Platform Options for Ethernet

Platform	Deployment Location Options
Cisco Industrial Ethernet 2000 Series Switches (IE2000)	• Station LAN, station WAN, and tank farms • DIN rail • Fixed form factor • Layer 2 only • Ruggedized for harsh environments
Cisco Industrial Ethernet 3000 Series Switches (IE3000)	• Station LAN, station WAN, and tank farms • DIN rail • Layer 2 and Layer 3 • Modular • Ruggedized for harsh environments
Cisco Industrial Ethernet 4000 Series Switches (IE4000)	• Station LAN, station WAN, aggregation • DIN rail • Fully Gigabit fixed form factor • Layer 2 and Layer 3 • Ruggedized for harsh environments
Cisco Industrial Ethernet 3010 (IE3010) and Cisco 2520 Connected Grid Switch (CGS2520)	• Station LAN, station WAN, and aggregation sites • 19-inch rack-mount • Layer 2 and Layer 3 • Ruggedized for harsh environments
Cisco ME 3400E Series Ethernet Access Switches	• Station WAN and aggregation sites • 19-inch rack-mount • Layer 2 and Layer 3 • Conditioned environments
Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000)	• Control center • Various 19-inch rack-unit (19RU) mounting options • Embedded high-speed firewall

IP/MPLS and MPLS-TP

MPLS provides highly scalable and secure VPNs, end-to-end QoS, and high availability, enabling efficient use of converged network infrastructure to meet the current and future growth needs of pipeline operators rather than separately deployed and managed infrastructure.

Multiprotocol Label Switching Transport Profile (MPLS-TP) is a transport-optimized protocol that has a subset of the full IP/MPLS feature set that is defined in the IETF. It is a simplified version of MPLS for transport networks with some of the MPLS functions turned off, offering an evolution architecture for time-division multiplexing (TDM)-based transport networks, and is optimized to carry packets.

MPLS delivers numerous benefits (Figure 7):

- Predictability of performance, support for DiffServ, monitorable SLAs, and end-to-end management
- Facilitation of the integration of multiple operational and multiservice applications over a common infrastructure, helping reduce capital expenditures (CapEx) and operating expenses (OpEx)
- Strong traffic-engineering capability providing deterministic application behavior and helping ensure one service does not affect another
- Station-to–control center security and privacy
- Rich hierarchical QoS mechanisms with simultaneous support for multiple operational and multiservice applications
- Scalability of bandwidth, services, and site connections allowing quick and easy deployment of new applications

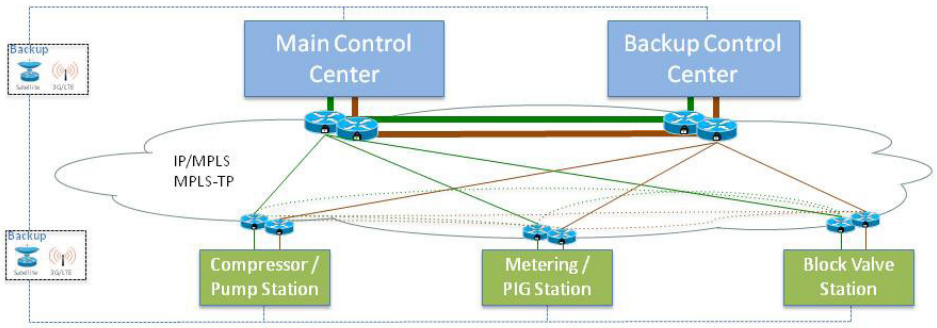

Figure 7. High-Level MPLS-Based Pipeline Architecture

Many architectural and technical areas should be considered when deploying an MPLS-based WAN for pipeline operations, as highlighted in Table 5. The skill sets and training of support personnel should also be considered.

Table 5. Technical Considerations When Deploying MPLS

Benefits and Considerations
Scalability and ease of deploying new services; scaling to hundreds or thousands of sites supporting multiple operational and multiservice applications, with simple new service introduction
Granular and flexible QoS model to ensure applications receive the correct bandwidth, latency, and jitter to ensure optimal performance in a flexible manner
Traffic path selection on a per-application basis to provide optimized traffic flow for critical applications
MPLS Fast Reroute (FRR) for network convergence <50 ms, providing fast path-failure recovery, and traffic engineering to provide deterministic application flow across the WAN
The option that the operator's choice of Layer 3 routing protocols such as OSPF, EIGRP, and IS-IS can be run across the Ethernet WAN to support all operational and multiservice applications
Comprehensive management options, and SLA monitoring for network performance
End-to-end logical proven security options through Layer 2 or Layer 3 VPNs from the control center to the pipeline station, providing effective use of fiber pairs where logical separation can be employed
Transport of older or traditional SCADA protocols through TCP Raw Sockets or CESoPSN/SAToP pseudowire
Increasing skill sets for implementation and ongoing management and administration, particularly as IT and operational technology (OT) are working together to deliver solutions, and use of service provider training to optimize skill sets
Distance limitation between stations, 80 km maximum, for connectivity without additional technologies

The technology platform choice for an MPLS-based WAN will again depend on environmental, power, and space requirements, as well as technology preference by the pipeline operator (Table 6).

Table 6. Recommended Platform Options for MPLS

Platform	Deployment Location Options
Cisco ASR 920	• Station WAN and aggregation sites • 1RU fixed form factor • Extended temperature support
Cisco ASR 903	• Station WAN and aggregation sites • 3RU 19-inch rack-mount • Modular • Fully redundant • Ruggedized for harsh environments • Older interface support • TDM integration
Cisco ASR 902	• Station WAN and aggregation sites • 2RU 19-inch rack-mount • Modular • Extended temperature support

Platform	Deployment Location Options
Cisco 2010 Connected Grid Router	• Station WAN and aggregation sites • 2RU 19-inch rack-mount • Ruggedized for harsh environments • Firewall services • Older interface support
Cisco Metro Ethernet 3600X and 3800X Series	• Station WAN and aggregation sites • 19-inch rack-mount • Layer 2 and Layer 3 • Conditioned environments
Cisco ASR 1000	• Control center • Various RU 19-inch rack-mount options • Advanced security features such as zone-based firewall and VPN encryption

DWDM

From both technical and economic perspectives, the ability to provide potentially unlimited transmission capacity over very long distances is the most obvious advantage of DWDM technology. Fiber investment can not only be preserved, but it also can be optimized by a factor of at least 32. In addition, it provides the following benefits (Figure 8):

- **Transparency:** Because DWDM is a physical layer architecture, it can transparently support Ethernet, IP, MPLS, and TDM technologies over a common physical layer as well as providing a migration path through interoperability with older TDM infrastructure.
- **Dynamic provisioning and ease of management:** Fast, simple, and dynamic provisioning of network connections allows you to turn on new services in days rather than months, with a comprehensive suite of planning and management tools available.
- **Reliability:** With extensive network performance analysis options and sub-50-ms path protection, pipeline application can operate reliably.
- **Long-distance connectivity:** Services can be extended over thousands of kilometers, meeting the requirements of pipelines where stations are further than 80 km apart, or where services need to be extended point-to-point for specific locations.
- **New revenue opportunities:** Pipeline operators can provision services rapidly by providing wavelength-on-demand services and leasing for external service providers.

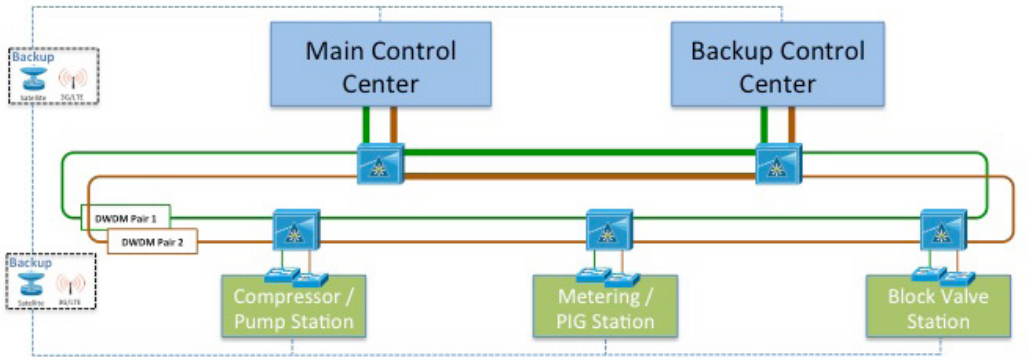

Figure 8. High-Level DWDM-Based Pipeline Architecture

Many architectural and technical areas should be considered when deploying a DWDM-based WAN for pipeline operations, as highlighted in Table 7. The skill sets and training of support personnel should also need be considered.

Table 7. Technical Considerations for DWDM Deployments

Benefits and Considerations
Scalable high bandwidth to support current and future services
High-speed backbone transport, with expressway functions between stations and control centers; point-to-point, multipoint, and full mesh topologies
Effective use of limited fiber pairs with wavelength/lambda separation between traffic types
Ability to transparently carry IP, IP/MPLS, and Ethernet technologies, as well as TDM; the operator's choice of Layer 3 routing protocols such as OSPF, EIGRP, and IS-IS can be run across the Ethernet WAN to support all operational and multiservice applications
Comprehensive management options, and SLA monitoring for network performance
End-to-end proven security options through wavelength/lambda separation, from control center to pipeline station
Sub-50-ms path protection for resiliency and high availability
Removal of distance limitations with possibilities to reach 3000 km
Ease of deployment for new services by turning on a new wavelength
Increasing skill sets for implementation and ongoing management and administration, particularly as IT and OT are working together to deliver solutions, and ability to use service provider training to optimize skill sets

The technology platform choice for a DWDM-based WAN will again depend on environmental, power, and space requirements, as well as technology preference by the pipeline operator (Table 8).

Table 8. Recommended Platform Options for DWDM

Platform	Deployment Location Options
Cisco ONS 15454 Multiservice Provisioning Platform	• Station WAN and aggregation sites • 2RU, 6RU, and 12RU 19-inch rack-mount modular platforms • TDM integration • Conditioned environments
Cisco Carrier Packet Transport (CPT) 50, 200, and 600	• Station WAN and aggregation sites • 1RU, 2RU, and 6RU 19-inch rack-mount modular platforms • TDM integration • Conditioned environments
Cisco ASR 903	• Station WAN and aggregation sites • 3RU 19-inch rack-mount • Modular • Fully redundant • Ruggedized for harsh environments • Older interface support • TDM integration

Nonwired

For brownfield retrofit in areas where fiber is not available, and as backup to wired technologies, secure wireless or cellular-based services such as WiMAX, Third-Generation Mobile Network (3G), Long Term Evolution (LTE), and satellite are available. These technologies still allow the transport of Ethernet, IP, and MPLS, but with restricted capabilities because of bandwidth availability. Converged operational and multiservice application deployments are still possible, but detailed QoS design is essential to ensure operational traffic is given priority in normal operation, particularly if this option is a backup option.

The deployment of wireless and cellular technologies and wired in the same communications network infrastructure is also possible, and indeed essential in some areas where it is not practical or economically feasible to run fiber. Again careful consideration of the architecture is needed to maximize performance and ensure correct operation of the pipeline management systems (Figure 9)

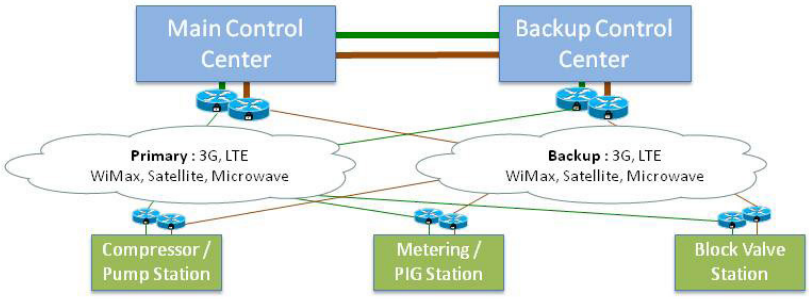

Figure 9. High-Level Wireless and Cellular-Based Pipeline Architecture

Numerous proven platforms are available to support wireless and cellular in a pipeline environment, as shown in Table 9. The choice will depend on environmental, power, and space requirements, as well as technology preference by the pipeline operator.

Table 9. Recommended Platform Options for DWDM

Platform	Deployment Location Options
Cisco 819H Router	• Station WAN • Ruggedized for harsh environments • Older interface support
Cisco 829 Industrial Integrated Services Router	• Station WAN • Ruggedized for harsh environments • Older interface support • Integrated firewall
Cisco 1000 Connected Grid Router (CGR1000)	• Station WAN • Indoor and outdoor models • Ruggedized for harsh environments • Older interface support • Native cellular and WiMAX
Cisco 2010 Connected Grid Router (CGR2010)	• Station WAN • Ruggedized for harsh environments • Older interface support • Modular with wired and wireless interface options
Cisco 3900 Series Integrated Services Router and Cisco ASR 1000 Aggregation Services Router	• Control center and aggregation sites • Conditioned environments

Table 10. Technology Overview

Technology	Bandwidth	Latency	Distance	Reliability	<50ms Re-convergence	QoS	Skillsets for Deploy/Operate	Multiservice Support
Ethernet	●	●	●	●	●	●	●	●
MPLS	●	●	●	●	●	●	●	●
DWDM	●	●	●	●	●	N/A	●	●
3G	●	●	●	●	●	●	●	●
LTE	●	●	●	●	●	●	●	●
Satellite	●	●	●	●	●	●	●	●
WiMax	●	●	●	●	●	●	●	●

The technology choice implemented will vary because of many reasons mentioned, including customer preference, power and space availability, capital and operational costs, architectural design, and validated testing (Table 10). Mixed environments are also likely with two or more technology choices used as part of the same design. As an example, DWDM may be implemented in larger pipeline stations where power and cooling are typically not challenges, providing a high-speed, high-bandwidth backbone across the pipeline. In block valve stations DWDM cannot be deployed because of power and space constraints, or lack of fiber, and therefore an alternative technology such as 3G or LTE may be deployed. Whatever technology choice is implemented, the foundation architecture is essential to ensure ease of implementation and operation of the communication networks and the pipeline management systems.

Security Appliances

To ensure secure remote access, Industrial DMZ (L3.5 DMZ) traversal, segregation and zoning, and intrusion prevention and detection, security appliances are deployed at the Control Centre head-end and in the pipeline stations where appropriate.

In the Control Centre a more powerful non-ruggedized appliance would typically be deployed due to performance and scalability requirements, while in the stations a hardened small form factor appliance would typically be needed.

Table 11.

Cisco 5500-X Series Firewalls	• Control Centre, large pipeline station • Separation between process control domain and enterprise
Cisco ISA-3000 Industrial Security Appliance	• Pipeline station • DIN rail • Ruggedized for harsh environments

Chapter 6

Key Pipeline Communication Deliverables

Irrespective of operational field telecoms' technology choice, key requirements must be considered to ensure optimal performance:

- **Predictable performance:** The ability to ensure that a packet is sent and received in a specific period of time is an important design goal for pipeline networks. For the network to support predictable, real-time traffic, the design must be as simple and highly structured as possible.
- **DiffServ:** A pipeline network will transmit many traffic types, from routine data to critical control information, or even bandwidth-intensive security video or collaborative voice services. The network must be able to distinguish between, and give priority to, different types of traffic. By doing so the network can deliver real-time network services with low latency and jitter, and minimal packet loss when the network infrastructure is under load. This capability to share the network with other applications, yet maintain the priority of the critical traffic, is a key requirement for pipeline operation.
- **Standardization:** A key development in industrial networks is the need to standardize around a common infrastructure using standardized protocols. Unlike proprietary technologies that may tie companies to a particular vendor, standardized solutions free users to choose the best application for a given solution.
- **Network management and diagnostics:** Management and diagnostics involves tools, applications, and devices used to monitor and maintain a network. Although a typical pipeline network does not drastically change after deployment, the network needs to be maintained and managed. Historically, these functions have not been incorporated into the automation and control systems, but this paradigm is changing. Today the networks and the telecoms system should be considered part of the whole pipeline process because they represent a key factor in the success of the project. Therefore, network design and architecture must include how the network will be managed and what tools, training, and resources are required to put them in place. A critical factor when resolving a problem over a widely distributed pipeline network is having the right information. This information enables personnel to monitor and maintain the network infrastructure as they do with the other automation and control equipment in order to optimize the whole pipeline operation. The key functions of network management as defined by the International Organization for Standards (ISO) are listed in Table 12.

Table 12. Functions of Network Management

Function	Description
Performance management	Gathering, analyzing, and reporting on key network variables including device and link availability, throughput and usage, and user response time
Configuration management	Managing and updating network configurations including operating system versions and network parameters (port, switch, and router settings)
Accounting management	Management of user and device accounts on the network
Fault management	Detection, logging, and notification to administrators of problems or faults within the network
Security management	Control of access to the network and monitoring of the network traffic for security threats and breaches

- **Network cyber security:** Technology can provide not only excellent performance for oil and gas applications, but also a wide range of network security measures to maintain availability, integrity, and confidentiality of the automation and control systems. Availability is most often cited as the key security requirement, keeping the automation and control systems operational. Integrity protects data and systems from intentional or accidental alteration. Confidentiality helps ensure that data cannot be accessed by unauthorized users. These network security advantages protect operational and multiservice assets. Security is maintained through a lifecycle of design, implementation, maintenance, and improvement. Security and administration policies, as well as periodic network audits, are a key foundation for developing robust network security.
- **Reliability:** Pipeline operations applications and services run in real or near real time, 24 hours a day excluding maintenance windows; the network must be available to users on a continuous basis, with little or no downtime. A communications network should be architected using effective network design principles, as well as intelligent networking services.
- **Real-time traffic performance:** Pipeline operations rely on effective pipeline management systems, and the network must be optimized to deliver consistent performance. To achieve this level of performance, technologies that prioritize and filter traffic and segment the network need to be part of the network design. Data must be prioritized using QoS to ensure that critical application information is received first. Operational devices and controllers must also be grouped appropriately to optimize data flow and effectively traverse the WAN.
- **Power availability and equipment footprint:** Depending on the location of the pipeline stations and the customer or end-user preference, power and space may be limited, and this limitation can affect the type of equipment and communications technologies that are available.

Chapter 7

Conclusion

By following an integrated architecture for pipeline operations and telecoms infrastructure, it is possible to create a modern converged operational and multiservice WAN supporting a choice of the latest wired and wireless technologies. This model enables secure backhaul, optimized services, reliability, and resiliency not previously available in traditional pipeline infrastructures, allowing operators to realize the following benefits:

- **CapEx savings:** Innovative integrated enterprise pipeline SCADA with pipeline operations applications, controllers, and RTUs, and telecoms infrastructure supporting multiservice applications result in engineering cost savings through enhanced integration, and lower total installation costs through centralized project management.
- **OpEx savings:** These savings are realized through energy management and efficiency, maintenance optimization through remote monitoring, and reduced communications network complexity to manage.
- **Enhanced pipeline safety and reliability:** Safety and reliability are enhanced with immediate response to leaks without false alarms, integrated security, secure power and reliable electrical distribution, and redundancy at all levels (control centers, SCADA servers, controllers, telecoms for operational field, and pipeline stations).
- **Regulatory compliance with enhanced productivity:** Embedded safety features help ensure regulatory compliance and operations efficiency.
- **Physical and cyber security challenges:** A converged network that provides cyber security detection and mitigation, video surveillance, and access control improves security and risk management through end-to-end application visibility and control.
- **Reduced power consumption:** Power-optimization technology reduces costs and energy consumption when running a pipeline, with the benefit of reduction in carbon emissions.
- **Efficient real-time pipeline operations:** A complete and integrated suite of advanced gas and liquids applications improves operational control, monitoring, and planning. Information management and business reporting allows for critical and comprehensive information with a minimum of effort.

- **Better infrastructure manageability and visibility:** Infrastructure manageability and visibility are better for both operational and multiservice applications, helping ensure continued pipeline operations by identifying and resolving communications challenges before they happen, or rapidly fixing them if they occur.
- **More efficient business processes for better financial and commercial governance:** Accurate liquids and gas-flow measurement data supports accurate customer billing through coupling commercial transaction technology, automated critical accounting, and reporting tasks.
- **Platform for new services:** Operational and multiservice applications continue to develop in the oil and gas industry. Through a planned architecture providing multiple technology choices, new services can be deployed quickly and easily.
- **More efficient business processes for better financial and commercial governance:** Accurate liquids and gas-flow measurement data supports accurate customer billing through coupling commercial transaction technology, automated critical accounting, and reporting tasks.

Chapter 8

Contributors

Serhii Konovalov: Oil & Gas Vertical Lead, IoE Vertical Solutions Group, Cisco Systems

Rodrigo Kaschny: Oil & Gas StruxureLabs Director, Smart Infrastructure, Schneider Electric

Anthony Napolitano: Technical Leader, Enterprise Pipeline Management Solutions, Schneider Electric

Alan Acquatella: Director Oil&Gas Solutions Midstream, Schneider Electric

Jean Noel Enckle: Partner Alliance Manager, ISGE, Cisco Systems

Jose Manuel Peinado Aguilar: Telecom Solution Architect, Energy Application Center, Schneider Electric

Chapter 9

Glossary

1PPP: 1 pulse per second

3G: Third-Generation Mobile Network

CAPEX: Capital expenditures

CCTV: Closed-circuit television

DNP3: Distributed Network Protocol

DWDM: Dense wavelength-division multiplexing

EIGRP: Enhanced IGRP

FTP: File Transfer Protocol

GOOSE: Generic Object Oriented Station Event

IEC: International Electrotechnical Commission

IPICS: IP Interoperability and Collaboration System

IS-IS: Intermediate System-to-Intermediate System

KPI: Key performance indicator

LTE: Long Term Evolution

MMS: Manufacturing Message Specification

MPLS: Multiprotocol Label Switching

MPLS-TP: MPLS - Transport Profile

NTP: Network Time Protocol

OLE: Object Linking and Embedding

OPC: OLE for Process Control

OPEX: Operating expenses

OTN: Optical Transport Network

OSPF: Open Shortest Path First

PAGA: Public Address and General Alarm System

PIG: Pipeline Inspection Gauge

PSOM: Cisco Physical Security Operations Manager

PTP: Precision Time Protocol

REP: Resilient Ethernet Protocol

SCADA: Supervisory Control and Data Acquisition

SLA: Service-level agreement

SNTP: Simple Network Time Protocol

SV: Sampled value

TDM: Time-division multiplexing

VoIP: Voice over IP

VSOM: Video Surveillance Operations Manager

Chapter 10

Additional Resources

- **Schneider Pipeline Management Solution:** http://www.schneider-electric.com.co/documents/local/xperience-efficiency/Pipeline_Management_Solution.pdf
- **Schneider—Best Practices in Leak Detection:** http://www.slideshare.net/SchneiderElectric/multi-tiered-leak-detectiona42013-25743519
- **Extending MPLS Across the End-to-End Network—Cisco Unified MPLS:** http://www.cisco.com/c/en/us/products/collateral/optical-networking/carrier-packet-transport-cpt-system/white_paper_c11-656286.pdf
- **Cisco MPLS WAN Design Guide:** http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2013/CVD-MPLSWANDesignGuide-DEC13.pdf
- **Cisco Layer 2 WAN Design Guide:** http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2013/CVD-Layer2WANDesignGuide-DEC13.pdf
- **Cisco—Understanding MPLS-TP:** http://www.cisco.com/en/US/technologies/tk436/tk428/white_paper_c11-562013.html
- **Cisco Introduction to DWDM:** http://www.cisco.com/web/AT/assets/docs/dwdm.pdf
- **Cisco Secure Operations Solution:** http://www.cisco.com/web/strategy/docs/energy/c45_732101_00_secure_ops_aag.pdf
- **Distributed optical acoustic sensing for pipeline monitoring:** http://www.pipelineandgasjournal.com/distributed-acoustic-sensing-pipeline-monitoring
- **Cisco ONS 15454 M6 data sheet:** http://www.cisco.com/c/en/us/products/optical-networking/ons-15454-m6-multiservice-transport-platform-mstp/index.html
- **Cisco ONS 15454 M2 data sheet:** http://www.cisco.com/c/en/us/products/optical-networking/ons-15454-m2-multiservice-transport-platform-mstp/index.html
- **Cisco IE 3000 data sheet:** http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-3000-series-switches/data_sheet_c78-440930.html
- **Cisco IE 2000 data sheet:** http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-2000-series-switches/datasheet-c78-730729.html
- **Cisco IE 3010 data sheet:** http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-3010-series-switches/datasheet_c78-637080.html
- **Cisco ME3 400E data sheet:** http://www.cisco.com/c/en/us/products/collateral/switches/me-3400e-series-ethernet-access-switches/data_sheet_c78-495220.html
- **Cisco ASR 903 data sheet:** http://www.cisco.com/c/en/us/products/collateral/switches/me-3400e-series-ethernet-access-switches/data_sheet_c78-495220.html
- **Cisco ASR 920 data sheet:** http://www.cisco.com/c/en/us/products/collateral/routers/asr-920-series-aggregation-services-router/datasheet-c78-732103.html?cachemode=refresh

c11-732758-02 1/16